ORDER FOR SUPPLIES AND SERVICES				IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution	PAGE 1 OF 2 PAGE(S)
1. DATE OF ORDER 04/23/2015	2. ORDER NUMBER GSQ1115BJ0014			3. CONTRACT NUMBER GS-06F-0711Z	4. ACT NUMBER A24739655

FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 299X	ORG CODE A11VR11I	B/A CODE FI	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE C01	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT

7. TO: CONTRACTOR *(Name, address and zip code)*	8. TYPE OF ORDER B. DELIVERY	REFERENCE YOUR
Payal Tak TELESIS CORPORATION 8300 GREENSBORO DRIVE SUITE 600 MCLEAN, VA 22102 United States 240-241-5610	Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.	
	This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.	
	C. MODIFICATION NO. 000 TYPE OF MODIFICATION:	AUTHORITY FOR ISSUING

9A. EMPLOYER'S IDENTIFICATION NUMBER (b) (6)	9B. CHECK, IF APPROP WITHHOLD 20%	Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.
10A. CLASSIFICATION A2. Woman Owned Business		10B. TYPE OF BUSINESS ORGANIZATION C. Corporation

11. ISSUING OFFICE *(Address, zip code, and telephone no.)*	12. REMITTANCE ADDRESS *(MANDATORY)*	13. SHIP TO *(Consignee address, zip code and telephone no.)*
GSA Region 11 Raina Baker 301 7th Street, SW Washington, DC 20407-0000 United States 202-708-6100	TELESIS CORPORATION 4700 CORRIDOR PL STE D ROCKVILLE, MD 20852-1631 United States	(b) (6) 550 12th Street, SW Washinton, DC 20024-0000 United States (b) (6)

14. PLACE OF INSPECTION AND ACCEPTANCE	15. REQUISITION OFFICE *(Name, symbol and telephone no.)*
(b) (6) 550 12th Street, SW Washinton, DC 20024-0000 United States	Julius S Bradshaw GSA Region 11 301 7th D S.W. WASHINGTON, DC 20407-0001 United States 202-708-5933

16. F.O.B. POINT	17. GOVERNMENT B/L NO.	18. DELIVERY F.O.B. POINT ON OR BEFORE	19. PAYMENT/DISCOUNT TERMS
Destination		05/14/2016	NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS

20. SCHEDULE

TASK ORDER AWARD FOR INFORMATION TECHNOLOGY CYBER SECURITY SERVICES ON BEHALF OF THE GOVERNMENT NATIONAL MORTGAGE ASSOCIATION.

FUNDING IN THE AMOUNT OF $1,740,610.72 IS HEREBY OBLIGATED TO FUND THE ENTIRE BASE PERIOD OF PERFORMANCE.

BASE PERIOD: 5/15/15-5/14/16
OPTION PERIOD I: 5/15/16-5/14/17
OPTION PERIOD II: 5/15/17-5/14/18
OPTION PERIOD III: 5/15/18-5/14/19
OPTION PERIOD IV: 5/15/19-5/14/20

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	PROJECT MANAGMENT - BASE PERIOD	1	lot	(b) (4)	
0002	SYSTEM SECURITY - BASE PERIOD	1	lot		
0003	ADMINISTRATIVE SUPPORT - BASE PERIOD	1	lot		
0004	TRANSITION-IN	1	lot		
0005	COST REIMBURSABLE TRAVEL - BASE PERIOD	1	lot		
0006	CONTRACT ACCESS FEE	1	lot		
0007	COST REIMBURSABLE (ODC) - BASE PERIOD	1	lot		

21. RECEIVING OFFICE *(Name, symbol and telephone no.)* GOVERNMENT NATIONAL MORTGAGE ASSOCIATION, 202-475-4975		TOTAL From 300-A(s)	
22. SHIPPING POINT Specified in QUOTE	23. GROSS SHIP WT.	GRAND TOTAL	$1,740,610.72
24. MAIL INVOICE TO: *(Include zip code)* General Services Administration (FUND) The contractor shall follow these Invoice Submission Instructions. The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).	25A. FOR INQUIRIES REGARDING PAYMENT CONTACT: GSA Finance Customer Support	25B. TELEPHONE NO. 816-926-7287	
	26A. NAME OF CONTRACTING/ORDERING OFFICER *(Type)* Raina Baker	26B. TELEPHONE NO. 202-708-6100	
	26C. SIGNATURE (b) (6)		
GENERAL SERVICES ADMINISTRATION	1. PAYING OFFICE	GSA FORM 300 (REV. 2-93)	

C.1 BACKGROUND

The Government National Mortgage Association (Ginnie Mae or GNMA) currently has a technology platform that resides in two separate vendor environments, Bank of New York for Integrated Pool Management System (IPMS) and The Navisite facility.

The IPMS makes past through payments to the Ginnie Mae investors and is the backbone of the Pay Processing Agent/Central Processing and Transfer Agent (PPA/CPTA) contract. Its primary function is to make the monthly past thru payments to all of the Ginnie Mae investors worldwide, which can result in payments in excess of $35 Billion monthly.

The Managed Data Center at the Navisite Facility hosts the Mortgage Backed Security Administration (MBSA) and the Ginnie Mae Financial Accounting System (GFAS) is hosted at the Managed Data Center located at the Navisite Facility. The Managed Data Center is contracted directly with Ginnie Mae and serves as its Managed and Hosted Services Data Center Provider. The Managed Data Center is responsible for the management and support of the technology infrastructure. The MBSA application includes Reporting and Feedback System (RFS), Corporate Watch and Issuer Scorecard (CWIS), SAS software, GinnieMae.Gov website and GFAS.

C.1.1 PURPOSE

Ginnie Mae has a requirement to obtain professional Information Technology (IT) Cyber Security services for the implementation and maintenance of Ginnie Mae's Enterprise Information Systems Security Program. This requirement will support ongoing efforts in providing assistance in the execution of the Chief Information Security Officer's security related responsibilities as well as the implementation of information assurance initiatives.

C.1.2 AGENCY MISSION

GNMA is a wholly owned corporate instrumentality of the US within the Department of Housing and Urban Development (HUD). Its authority is generally prescribed in Title III of the National Housing Act, as amended (12 U.S.C. 1716 et seq.). Through its Mortgage Backed Securities (MBS) programs, Ginnie Mae guarantees privately issued securities backed by pools of mortgages insured or guaranteed by the Federal Housing Administration (FHA), the Department of Veterans Affairs (VA), the Rural Housing Service of the Department of Agriculture (RHS), or HUD's Native American Program (PIH). Ginnie Mae guarantees the registered holder of the securities the timely payment of scheduled monthly principal and interest payments, loan prepayments and early recoveries of principal on the underlying mortgages.

C.2 SCOPE

The Contractor shall provide support services which entail services such as Continuity Of Operations Planning (COOP) disaster management, customer support, security scanning, network assessment and Security Assessment and Authorization review. The scope of the work will include:

- Network Scanning
- Application Scanning
- Plan of Action and Milestone tracking
- Penetration Testing
- Program and Project Management
- Disaster Recovery Testing
- Audit Reporting
- Network Engineering
- Security Engineering
- Cyber Security
- Risk Management

Additionally, the contractor will be required to travel to the 6 Ginnie Mae data centers at least twice per year to conduct scans, network penetration testing and audits in accordance with the Statement of Work.

C.3 CONSTRAINTS

The work identified in this task order will adhere to the rules, regulations, laws, standards and conventions identified by HUD/Ginnie Mae as well as within the federal Government. Constraints include but are not limited to the following:

Document Number	**TITLE**	Released	Mandatory (M) /Advisory (A)
44 USC §3541 et seq.	Federal Information Security Management Act (FISMA, supersedes the Computer Security Act of 1987)	2002	M
44 USC §3601 et seq.	E-Government Act of 2002	2002	M
Pub. L. 97-255, 31 USC §3512	Federal Managers' Financial Integrity Act (FMFIA) http://www.whitehouse.gov/omb/financial/fmfia1982.html	1982	M
Pub. L. 104-208, 31 USC 3512	Federal Financial Management Improvement Act of 1996 http://www.whitehouse.gov/omb/financial/fm_systems.html	1996	M
Pub. L. 104-106, 40 USC §1401 et seq.	Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)	1996	M
Pub. L. 105-277, 44 USC §3504	Government Paperwork Elimination Act http://www.whitehouse.gov/omb/fedreg/gpea2.html	1998	M
Pub. L. 105-220, 29 USC 701 et seq.	Section 508 of the Rehabilitation Act of 1998	1998	M
Pub. L. 97-177, 31 USC §3901 et seq.	Prompt Payment Act	1982	M
Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101	Title III (Federal Information Security Management Act of 2002)	2002	M

Document Number	**TITLE**	Released	Mandatory (M) /Advisory (A)
OMB Circular A-11, Part 3	"Planning, Budgeting, and Acquisition of Capital Assets" http://www.whitehouse.gov/omb/circulars/index.html	Latest version	M
OMB Circular A-123	Management Accountability and Control http://www.whitehouse.gov/omb/circulars/a127/a127.html	Latest version	M
OMB Circular A-125	OMB Circular A-125, Prompt Pay http://www.whitehouse.gov/omb/circulars/index.html	Latest version	M
OMB Circular A-127	Policies and Standards for Financial Management Systems http://www.whitehouse.gov/omb/circulars/a127/a127.html	Latest version	M
OMB Circular A-130	"Security of Federal Automated Information Resources" (Appendix III) http://www.whitehouse.gov/omb/circulars/index.html	Latest version	M
OMB Circular A-130	Management of Federal Information Resources http://www.whitehouse.gov/omb/circulars/index.html	Latest version	M
OMB Circular A-130	"Security of Federal Automated Information Resources" (Appendix III) (see also 34 FR 6428) http://www.whitehouse.gov/omb/circulars/index.html	Latest version	M
OMB Memorandum 99-20	"Security of Federal Automated Information Resources" http://www.whitehouse.gov/omb/memoranda/index.html	1999	M
OMB Memorandum 06-15	"Safeguarding Personally identifiable Information" http://www.whitehouse.gov/omb/memoranda/index.html	2006	M
OMB Memorandum 06-16	"Protection of Sensitive Agency Information" http://www.whitehouse.gov/omb/memoranda/index.html	2006	M
OMB Memorandum 06-19	"Reporting Incidents Involving PII" http://www.whitehouse.gov/omb/memoranda/index.html	2006	M
OMB Memorandum 06-20	"Reporting Instructions for the Federal Information Security Act and Agency Privacy Management" http://www.whitehouse.gov/omb/memoranda/index.html	2006	M
PDD-63	"Critical Infrastructure Protection," Presidential Decision Directive-63	1998	M
HSPD-12	"Policy for a Common Identification Standard for Federal Employees and Contractors," Home Security Presidential Directive-12	2004	M
NIST Special Publication 800-12	"An Introduction to Computer Security: The NIST Handbook"	Oct 1995	M
NIST Special Publication 800-14	"Generally Accepted Principles and Practices for Securing Information Technology Systems"	Sep 1996	M
NIST Special Publication 800-18	"Guide for Developing Security Plans for Federal Information Systems"	Feb 1996	A
NIST Special Publication 800-26	"Security Self-Assessment Guide for Information Technology Systems"	Nov 2001	M

Document Number	**TITLE**	Released	Mandatory (M) /Advisory (A)
NIST Special Publication 800-26, Rev. 1	"Guide for Information System Assessments and Program Reporting "	TBD	A
NIST Special Publication 800-30	"Risk Management Guide for Information Technology Systems"	Jul 2002	M
NIST Special Publication 800-34	"Contingency Planning Guide for Information Technology Systems"	Jun 2002	M
NIST Special Publication 800-35	"Guide to Information Technology Security Services"	Oct 2003	M
NIST Special Publication 800-37 Rev 1	"Guide for the Security Certification and Accreditation of Federal Information Systems"	Rev 1	M
NIST Special Publication 800-47	"Security Guide for Interconnecting Information Technology Systems"	Aug 2002	A
NIST Special Publication 800-53A	"Recommended Security Controls for Federal Information Systems"	Feb 2005	A
NIST Special Publication 800-53, Rev. 3 and 4	"Recommended Security Controls for Federal Information Systems"	April 2013	A
NIST Special Publication 800-55	"Security Metrics Guide for Information Technology Systems"	Jul 2003	A
NIST Special Publication 800-60	"Guide for Mapping Types of Information and Information Systems to Security Categories"	Jun 2004	A
NIST Special Publication 800-64	"Security Considerations in the Information System Development Life Cycle"	Oct 2003	A
NIST Special Publication 800-65	"Integrating Security into the Capital Planning and Investment Control Process"	Jan 2005	A
NIST Draft Special Publication 800-80	"Guide for Developing Performance Metrics for Information Security"	TBD	A
NIST Special Publication 800-100	"Information Security Handbook: A Guide for Managers"	Oct 2006	A
NIST SP 800-118	Guide to Enterprise Password Management		M
Fed-GAAP	Federal-based GAAP Compliant Summary Transactions www.fasab.gov/concepts.htm		M
General Accounting Office, GAO-02-45	HUD MANAGEMENT: Progress Made on Management Reforms, but Challenges Remain	October 2001	A

Document Number	TITLE	Released	Mandatory (M) /Advisory (A)
GAO/AIMD-00-33	"Information Security Risk Assessment Practices of Leading Organizations"	Nov 1999	A
Fed-GAAP	Federal-based GAAP Compliant Summary Transactions www.fasab.gov/concepts.htm		M
SSAE-16	(AICPA)		M
HSPD DIRECTIVE #7	Critical Infrastructure Identification, Prioritization, and Protection		M

C.3 OBJECTIVE

The objective of this requirement is to support on-going efforts in providing assistance in the execution of the chief information security officer security-related responsibilities and implementation of information assurance initiatives.

C.4 TASKS

C.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.4.1.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the COR. The contractor shall provide the following at the Kick-Off meeting:

a. Transition-In Plan
b. Project Management Plan
c. Quality Control Plan (QCP)

C.4.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor PM shall develop and provide an MSR using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Government Technical Representative (GTR) and the COR. The MSR shall include the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).

C.4.1.3 SUBTASK 3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting with the GTR, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.4.1.4 SUBTASK 4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
e. Include the contractor's Quality Control Plan (QCP)

The contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP shall incorporate the Government's comments.

C.4.2 TASK 2 - TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities will be completed 45 calendar days after the start date of the order. The contractor shall propose a draft Transition-In Plan within five workdays of award.

C.4.3 TASK 3 -TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The

contractor shall have sufficient personnel on board during the 60 day Transition-Out Period. The contractor shall provide a Transition-Out Plan NLT 60 calendar days prior to expiration of the TO. The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.4.4 TASK 4 – SYSTEM SECURITY SERVICES

C.4.4.1 SUBTASK 1 – PENETRATION TESTING

The contractor shall conduct non-invasive penetration testing that attempts to compromise the integrity on all Ginnie Mae outward facing websites, specifically www.ginniemae.gov. The contractor shall identify methods for circumventing the security features and vulnerabilities of the Ginnie Mae outward facing websites and provide a report of the results to include material weaknesses and other significant deficiencies. This testing shall occur 6 times during each performance period.

C.4.4.2 SUBTASK 2 – PENETRATION TESTING (INTERNAL)

The contractor shall conduct internal penetration testing to analyze and evaluate attempts to compromise the application on all Ginnie Mae major applications to include RFS, GFAS, IPMS, UFS, GinnieNET, GMEP and Web Services. The contractor shall provide a report of the results, to include material weaknesses and other significant deficiencies. This testing shall occur 6 times during each performance period.

C.4.4.3 SUBTASK 3 – SECURITY SELF ASSESSMENT

The Contractor shall monitor and input the (Agency) Security Self-Assessment into the Department of Homeland School (DHS) Trusted Agent Tool in accordance with the NIST Special Publication 800-26. The Security Self-Assessment shall describe the current state of the Application and Network and specify if the system is being maintained in accordance with FISMA, NIST, OMB and HUD policies, procedures and regulations. The Security Self-Assessment shall be conducted on all 10 of the Ginnie Mae major and minor applications.

C.4.4.4 SUBTASK 4 – SYSTEM SECURITY REQUIREMENTS POLICY REVIEW

The Contractor shall review and evaluate the existing statement of system security requirements and make recommendations for revision and improvements. Upon review of the security requirements, the contractor shall determine if additional safeguards are required and submit written recommendations to the GTR on a monthly basis.

C.4.4.5 SUBTASK 5 – CONTROL MATRIX

The Contractor shall prepare a control matrix identifying complex security strategies and the control techniques that will evaluate threats, analyze vulnerabilities, and achieve security objectives. This matrix shall be reviewed and updated twice per quarter and shall not exceed 8 occurrences per year. Upon review of the control matrix, the contractor shall determine if additional safeguards are required and include findings in a written report to the GTR.

C.4.4.6 SUBTASK 6 – SECURITY AUTHORIZATION PACKAGE

The Contractor shall prepare a written security authorization package for all Ginnie Mae Contractor systems and services in accordance with NIST Special Publication 800-37 Rev1, Guide for the Security Certification and Accreditation of Federal Information Systems. The Security Authorization package shall be delivered to the Chief Information Security Officer for review on 10 separate occasions or as required for a system re-certification during each performance period. The authorization packages shall cover all 10 of the Ginnie Mae major and minor applications. The Security Authorization Package shall be prepared during the base period of performance and Option Period III.

The security authorization package shall contain at a minimum:

- The security accreditation decision letter, to be signed by the authorizing (Agency) official, conveying the accreditation decision
- Supporting rationale for the decision
- Any terms and conditions placed on the system owners
- Any supporting documentation related to the security certification and accreditation process that the authorizing official wishes to provide to the system owner
- Plan of Action and Milestones
- System Security Plan
- Risk Assessment

C.4.4.7 SUBTASK 7 – THREAT ASSESSMENT

The contractor shall perform a threat assessment for the Ginnie Mae Applications and Infrastructure environment on a quarterly basis. The assessment shall include an in depth analysis of the Application and Infrastructure environment to identify any known and unknown potential vulnerabilities to the specific environments. Upon completion of the assessment, the contractor shall provide a report which describes all potential vulnerabilities that may cause harm to the Ginnie Mae environment, along with recommended corrective actions.

C.4.4.8 SUBTASK 8 – APPLICATION & NETWORK CREDENTIALED SCANS

The Contractor shall perform application and network credentialed scans, on all Ginnie Mae environments and provide written results of the scans to the GTR. The contractor shall perform analysis to discover any business logic flaws that could become security defects as well as test and identify vulnerabilities within Ginnie Mae applications and networks. The frequency of the scans shall not exceed 10 occurrences during each performance period.

C.4.4.9 SUBTASK 9 – PLAN OF ACTION & MILESTONES (POA&M) REPORTS

The Contractor shall prepare and submit POA&M reports for the 10 Ginnie Mae major and minor applications on a quarterly basis to GTR. The POA&M Reports shall identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems. Additionally, the updated POA&M summary report shall be updated in the HUD CSAM database on a quarterly basis as required by The Office of Management & Budget (OMB) ensuring adherence to applicable FISMA and NIST regulations.

C.4.4.10 SUBTASK 10 – AUDITS

The Contractor shall conduct IT Security scans of network and/or application audits of Ginnie Mae service providers to include: Bank of New York, NaviSite and Deloitte. The contractor shall perform audits of the service providers on two separate occasions during the performance period. The contractor shall provide subsequent results of the audits to the Chief Information Security Officer, along with all supporting documentation in conjunction with Ginnie Mae audits on Ginnie Mae systems to include A-123 Audits, A-127 Audits, HUD IG Audits, GAO Audits, and OMB Audits.

C.4.4.11 SUBTASK 11 – SECURITY SUB-POLICIES AND PROCEDURES

The Contractor shall review and recommend updates to Ginnie Mae IT Security Sub-Policies and Procedures in order to ensure adherence to all HUD, FISMA, NIST and Ginnie Mae policies and regulations. A report of the review and subsequent recommendations shall be provided in writing on a quarterly basis to the GTR.

C.4.5 TASK 5 – ADMINISTRATIVE SUPPORT SERVICES

C.4.5.1 SUBTASK 1 – PRIVACY IMPACT ASSESSMENT

The Contractor shall perform a Privacy Impact Assessment in accordance with standard industry practices on a bi annual basis to ensure compliance with the Privacy Act. The assessment shall evaluate and analyze how personally identifiable information (PII) is collected, used, shared, and maintained within Ginnie Mae systems to determine if the PII is adequately protected. The Contractor shall provide the GTR all findings, supporting documentation and a written assessment of all data gathered during the Privacy Impact Assessment. The assessment shall include all 10 of the Ginnie Mae major and minor applications.

C.4.5.2 SUBTASK 2 – DATA PRIVACY ASSESSMENT

The Contractor shall perform data privacy assessment and provide the GTR with all findings and recommendations. The assessment shall occur on a bi-annual basis on all 10 of the Ginnie Mae major and minor applications during each performance period.

C.4.5.3 SUBTASK 3 – INFORMATION ASSURANCE SECURITY POLICIES

The Contractor shall perform analysis and develop Information Assurance Security Policies and Sub-policies during the term of the contract. The analysis of security policies and sub-policies shall occur on a bi annual basis during each performance period.

C.4.5.4 SUBTASK 4 – DISASTER RECOVERY

The Contractor shall monitor all disaster recovery tests of Ginnie Mae and non Ginnie Mae Information Technology systems on 6 separate occasions during the performance period. The Contractor shall document the results of the discovery tests as part of the security self-assessment to be submitted to Ginne Mae for review.

C.5 QUALITY ASSURANCE

The offeror shall institute and maintain the capability to ensure the quality of the services required under this task order. The contractor shall apply industry standards and best practices. Quality assurance practices in program management to include, at a minimum, identification of quality control factors and processes, evaluation methods, earned value, and process improvement.

The contractor shall prepare a Quality Control Plan (QCP) and perform quality control functions in accordance with the Plan. The contractor shall deliver quality control reports as described in the government-approved QCP. The QCP may be modified as the project progresses by coordinated approval of the contractor and the government.